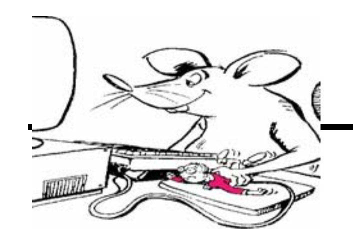


Chapter 9 الفصل التاسع
Viruses الفيروسات

الفيروسات و التهديدات ذات الصلة (Viruses and Related Threats)

- البرامج الخبيثة (Malicious Programs).
- طبيعة الفيروسات (The Nature of Viruses).
- مفاهيم مضادات الفيروسات (Antivirus Approaches).
- تقنيات مضادات الفيروسات المتقدمة (Advanced Antivirus Tech niques).

مقدمة :

- أن أغلب أنواع التهديدات على أنظمة الحاسوب تتمثل في البرامج التي تستغل نقاط الضعف في الأنظمة الحاسوبية.
- و سنركز في هذا السياق على برامج التطبيق (Application Programs) و البرامج المساعدة (Utility Programs) ، مثل : المحررات (editors) و المترجمات (compilers).

البرامج الخبيثة (Malicious Programs).

يقدم الشكل التالي تصنيفاً كلياً للتهديدات البرمجية (أو البرامج الخبيثة).
يمكن تصنيف هذه التهديدات إلى صنفين :

برامج خبيثة تحتاج إلى برنامج مضيف (Malicious programs need host program):

- في الأساس تكون عبارة عن أجزاء لبرامج لا يمكن أن توجد بشكل مستقل عن بعض برامج التطبيق الحقيقية، أو البرامج المساعدة، أو برامج النظام.

برامج خبيثة مستقلة (Independent malicious programs):

- هي برامج ذات محتوى ذاتي يمكن جدولتها و تشغليها من قبل نظام التشغيل.

و هناك تصنيف آخر لهذه التهديدات من حيث تكرارها لنفسها و عدم تكرارها:

برامج خبيثة لا تكرر نفسها (Non-replicate malicious programs):

- و هي عبارة عن أجزاء من برامج يتم تنشطيها عندما يتم نداء البرنامج المضيف لإنجاز عملية معينة.

برامج خبيثة تكرر نفسها (Replicate malicious programs):

- و هي تتكون من جزء من برنامج (virus) أو قد تكون برنامجاً مستقلاً (bacteria, worm).
- و عند تنفيذ هذه البرامج قد تنتج نسخة أو أكثر من نفسها بغرض تفعيلها في نفس النظام أو في نظام آخر.

- بإمكانك الاستعانة بالشكل التالي لفهم التصنيفات السابقة.
- و سنعتمد على هذا الشكل في تنظيم المعلومات التي سنناقشها.





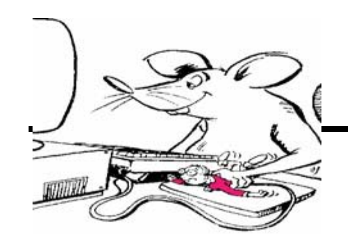
- Malicious Programs
  - Need Host Program
    - Trapdoors
    - Logic Bombs
    - Trojan Horses
    - Viruses
  - Independent
    - Bacteria
    - Worms

<u>الأبواب الخلفية (Trap Doors):</u>

- هو عبارة عن نقطة دخول سرية للبرنامج ، تسمح لأي شخص مدرك لهذا الـ (Trap door) أن يحصل على حق الوصول بدون المرور عبر إجراءات الوصول السرية.
- استخدمت قديماً لتنقيح و اختبار البرامج.
- تحولت الـ (Trap doors) إلى مهددات عندما استخدمت بواسطة المبرمجين عديمي الضمير و ذلك بغرض الحصول على وصول غير مصرح به.

<u>القنبلة المنطقية (Logic Bomb):</u>

هي واحدة من أقدم أنواع المهددات البرمجية، حيث أنها سبقت الـ (viruses) و الـ (worms).
و هي عبارة عن كود مضمن في برنامج شرعي يكون مضبوط في وضع الانفجار عند تحقق شروط معينة.
من الأمثلة على هذه الشروط (وجود أو غياب ملفات معينة) أو (الوصول إلى يوم معين من الأسبوع أو تأريخ محدد) أو (عندما يكون المستخدم شخص محدد).
يمكن لهذه القنبلة أن تغير أو تحذف البيانات أو حتى الملفات برمتها ، كذلك قد تسبب في توقف الآلة، أو حدوث أي دمار من نوع آخر.



أحصنة طروادة (Trojan Horses):

- هو عبارة عن برنامج أو أمر إجرائي ذو فائدة ، أو لنقل ذو فائدة ظاهرية.
- يحتوي هذا البرنامج على شفرة مخفية (hidden code).
- عندما يتم نداء هذه الشفرة، فإنها تقوم بعمليات غير مرغوبة و ضارة.
- يمكن استخدام برامج الـ (Trojan Horse) للقيام بالوظائف التي لا يمكن لمستخدم غير مصرح له بتنفيذها مباشرة و ذلك عن طريق تنفيذها بشكل غير مباشر (مثلاً، الحصول على حق الوصول لملفات مستخدم آخر في نظام مشترك).
- مثال على (Trojan Horse) لا يمكن اكتشافه:

الـ (compiler) الذي تم تعديله بحيث يدخل كود إضافي إلى برامج معينة أثناء دخولها في عملية الـ (compiling) ، مثل برنامج الدخول في النظام (system login program).
يقوم هذا الكود بعمل (trap door) في الـ (login program) و الذي يسمح للمصدر بأن يدخل النظام باستخدام كلمة مرور خاصة.
لا يمكن اكتشاف هذا الـ (Trojan Horse) عن طريق قراءة الكود المصدري للـ (login program).

- و هذه البرامج مدمرة للبيانات ، فبالرغم من ظهور البرنامج على أنه ينجز وظيفة مفيدة (مثل برنامج الحاسبة) لكنه في نفس الوقت يقوم بمسح لملفات المستخدم.

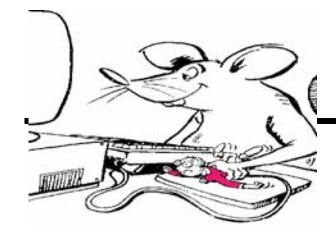
الفيروسات (Viruses):

- هو عبارة عن برنامج يمكنه أن "يعدي" برامج أخرى عن طريق تعديلها: و هذا التعديل يتضمن نسخة من برنامج الـ (Virus) و التي يمكنها بعد ذلك أن تعدي برامج أخرى.
- الفيروسات البيولوجية هي عبارة عن نفايات صغيرة جداً ناتجة من شفرة جينية (حامض الـ DNA أو الـ RNA)، و هي تتولى الآلية التي تنتهجها الخلية الحية و تقوم بخداعها بحيث تعمل الآلاف من النسخ للفيروس الأصلي و التي لا عيب فيها.
- الفيروسات الحاسوبية تحمل في شفرتها التعليمية الوصفة التي تتمكن من خلالها من عمل نسخة كاملة لنفسها.
- يتحكم الفيروس بشكل مؤقت بنظام تشغيل الأقراص (DOS)، و عندما يحصل أي اتصال بين الحاسوب المصاب بالعدوى و أي قطعة برمجية غير مصابة بالعدوى، فإن نسخة جديدة من الفيروس سوف تنتقل إلى البرنامج الجديد.
- و بالتالي، يمكن أن تنتشر العدوى من جهاز حاسوب إلى آخر بواسطة مستخدمين غير معنيين بعمليات الإضرار بالآخرين (عن طريق تبادل الديسكات أو إرسال الملفات عبر الشبكة).

الديدان (Worms):

- و هي برامج تستخدم الارتباطات الشبكية للانتشار من نظام إلى آخر.
- عندما تكون الدودة الشبكية (Network worm) مفعلة في نظامٍ ما، فإنها تعمل بشكلٍ مشابهٍ للفيروسات (Viruses) و البكتيريا (Bacteria) ، أو أنها قد تزرع برامج الـ (Trojan Horse) أو تقوم بعدد من الأحداث المزعجة و المدمرة.
- تستخدم الدودة الشبكية بعض أنواع المركبات الشبكية و ذلك بغرض مضاعفة نفسها، و من الأمثلة على ذلك:
  - ميزة البريد الالكتروني (Electronic mail facility):
    ترسل الدودة نسخة من نفسها إلى الأنظمة الأخرى عبر البريد الإلكتروني.
  - مقدرة التنفيذ عن بعد (Remote execution capability):
    تنفذ الدودة نسخة من نفسها في نظام آخر.





- مقدرة الدخول عن بعد (Remote login capability):
  تدخل الدودة في نظام بعيد كمستخدم و من ثم تستخدم أوامر لنسخ نفسها من نظام إلى آخر.
- تُظهر الدودة الشبكية نفس خصائص الفيروسات الحاسوبية:
  - طور الخمول (Dormant phase).
  - طور الانتشار (Propagation phase).
  - طور القدح (Triggering phase).
  - طور التنفيذ (Execution phase).
- طور الانتشار (Dormant phase) تتم فيه الوظائف التالية:
  - البحث عن أنظمة أخرى من أجل نقل العدوى إليها عن طريق فحص الـ (host tables) أو أي مستودعات مشابه لعناوين النظام البعيد.
  - تأسيس ارتباط مع النظام البعيد.
  - نسخ نفسها إلى النظام البعيد و تشغيل هذه النسخة.
- قد تحاول الدودة الشبكية أيضاً تحديد فيما إذا كان النظام قد أصيب بالعدوى سبقاً أم لا.
- كما هو الحال مع الفيروسات، فإن مواجهة الدودة الشبكية يعد أيضاً أمراً صعباً.

البكتيريا (Bacteria):

- و هي عبارة عن برامج لا تقوم بشكلٍ واضح بتدمير أي ملفات.
- الغرض الوحيد منها هو مضاعفة نفسها.
- برنامج البكتيريا العادي قد لا يقوم إلا بعملية نسختين من نفسه بشكلٍ متزامن في نظام برمجة متعددة.
- أو قد يقوم بخلق ملفين جديدين كلٌ منهما عبارة عن نسخة طبق الأصل لملف البكتيريا.
- كل هذه البرامج يمكنها بعد ذلك أن تنسخ نفسها مرتين، وهكذا.
- تحتل البكتيريا سعة المعالج و المساحة التخزينية في الذاكرة أو القرص، مما يعيق وصول لمستخدمين لهذه الموارد.

طبيعة الفيروسات (Nature of Viruses):

يمكن للفيروس أن يقوم بأي شيء تقوم به البرامج الأخرى.
الفرق الوحيد هو أن الفيروس يقوم بإلحاق نفسه ببرنامج آخر و التنفيذ بشكل سري عندما يتم تشغيل الـ (host program).
في حال تنفيذ الفيروس، فإن بإمكانه إنجاز أي وظيفة: مثل مسح الملفات و البرامج.

مراحل الدورة الحياتية للفيروس (Virus lifetime stages):

- طور الخمول (Dormant phase):
  - يكون الفيروس متعطلاً.
  - سيتم تنشيط الفيروس بواسطة حدث ما ، مثل (التأريخ ، وجود برنامج أو ملف آخر، تجاوز سعة الذاكرة لحد معين).
  - لا تمر كل الفيروسات بهذه المرحلة.
- طور الانتشار (Propagation phase):
  - يقوم الفيروس بوضع نسخة مطابقة له في برامج أخرى أو في مساحات نظام معينة داخل القرص.
  - كل برنامج سيحتوي على نسخة من الفيروس، و سيدخل بدوره في مرحلة الانتشار.





- طور القدح (Triggering phase):
  - يتم تنشيط الفيروس للقيام بالوظيفة التي عُمِل من أجلها.
  - كما هو الحال مع طور الخمول، يمكن أن يكون هناك أحداث مختلفة تؤدي إلى تفعيل هذا الطور، مثل (عدد المرات التي قام بها الفيروس بنسخ نفسه).
- طور التنفيذ (Execution phase):
  - يتم إنجاز الوظيفة.
  - قد تكون وظيفة الفيروس ضارة، مثل (رسالة على الشاشة) أو دمار، مثل (البرامج التدميرية و ملفات البيانات).

<u>بنية الفيروس (Virus structure):</u>

- يمكن أن يضاف الفيروس قبل أو بعد برنامج قابل للتنفيذ.
- العملية الأساسية في الفيروس هي أنه عندما يتم نداء البرنامج المصاب بالعدوى، فإن شفرة الفيروس هي التي ستنفذ أولاً ثم بعد ذلك ستنفذ شفرة البرنامج الأصلي.
- في الشكل التالي :
  - تم إضافة شفرة الفيروس، V، قبل البرامج المصابة بالعدوى.
  - تم افتراض أن نقطة الدخول للبرنامج عند نداءه هي أول سطر في البرنامج.
  - أول سطر في الكود سيقفز بنا إلى برنامج الفيروس الرئيسي.
  - السطر الثاني هو عبارة عن علامة خاصة يستخدمها الفيروس لتحديد فيما إذا كانت الضحية قد أصيبت بهذا الفيروس من قبل أم لا.
  - عندما يتم نداء البرنامج، ينتقل التحكم فوراً إلى برنامج الفيروس الرئيسي.
  - يبحث برنامج الفيروس أولاً عن ملفات قابلة للتنفيذ و يصيبها بالعدوى.
  - بعد ذلك قد يقوم الفيروس بعمل حدث معين. هذا الحدث يمكن أن يتم في كل مرة يتم فيها نداء البرنامج، أو قد يكون هذا الحدث عبارة عن (Logic Bomb) تطلق تحت شروطٍ معينة.
  - أخيراً، ينقل الفيروس التحكم إلى البرنامج الرئيسي.

```
program V :=

{goto main;
    1234567;

        subroutine infect-executable :=
            {loop:
            file := get-random-executable-file;
            if (first-line-of-file = 1234567)
                then goto loop
                else prepend V to file; }

        subroutine do-damage :=
            {whatever damage is to be done}

        subroutine trigger-pulled :=
            {return true if some condition holds}

main:   main-program :=
            {infect-executable;
            if trigger-pulled then do-damage;
            goto next;}

next:

}
```

